JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 9, No. 2, Juni 2024, Pp. 728-734

ANALISIS MANAJEMEN RISIKO INFORMASI MENGGUNAKAN ISO/IEC 27005:2018 (STUDI KASUS: PT.XYZ)

Muhammad Lukman Bahrul Hikam*[1)], Fitriyana Dewi[2)], Dhata Praditya[3)]
1. Telkom University, Indonesia
2. Telkom University, Indonesia
3. Telkom University, Indonesia

Article Info
Kata Kunci: ISO/IEC 27002:2022, ISO/IEC 27005:2018, *Risk Assesment,* SMKI

Keywords: *ISO/IEC 27002:2022, ISO/IEC 27005:2018, Risk Assesment, ISMS*

Article history:
Received 26 February 2024
Revised 11 March 2024
Accepted 25 March 2024
Available online 1 June 2024

DOI :
https://doi.org/10.29100/jipi.v9i2.4709

* Corresponding author.
Muhamamd Lukman Bahrul Hikam
E-mail address:
mlukmanbahrulhikam@student.telkomuniversity.ac.id

ABSTRAK
Risiko yang berkenaan dengan keamanan informasi perusahaan perlu untuk dikelola dengan baik karena informasi merupakan salah satu aset yang sangat berharga dalam menjalankan operasi bisnis. Pengelolaan risiko yang baik dapat membantu perusahaan untuk merencanakan pengendalian risiko supaya segala aset informasi yang dimiliki perusahaan tetap aman. Penelitian tentang manajemen risiko informasi pada PT. XYZ ini dilaksanakan dengan mengacu pada panduan ISO/IEC 27005:2018 tentang panduan praktik dalam mengelola risiko terhadap risiko informasi. ISO/IEC 27005 sendiri merupakan bagian dari keluarga ISO 27000 series yang yang mencakup panduan untuk penerapan SMKI (Sistem Manajemen Keamanan Informasi). Tujuan dari penelitian ini adalah untuk mengidentifiaksi potensi ancaman yang yang timbul dari kontrol keamanan informasi dari ISO/IEC 27002:2022 yang belum terpenuhi oleh PT. XYZ untuk selanjutnya akan dilakukan tahap *risk assesment* pada potensi ancaman utama. Hasil dari proses penilaian risiko didapatkan 7 potensi ancaman yang selanjutnya untuk masing masing ancaman diusulkan bentuk pengendalian risiko serta *action plan* nya. Hasil dari penelitian ini dapat digunakan sebagai referensi untuk melakukan analisis manajemen risiko informasi perusahaan terutama bagi ancaman risiko yang timbul dari tidak terpenuhinya kontrol keamanan pada standar ISO/IEC 27001.

ABSTRACT
Risks related to corporate information security need to be managed properly because information is one of the most valuable assets in carrying out business operations. Good risk management can help companies to plan risk control so that all information assets owned by the company remain safe. Research on information risk management at PT XYZ is carried out by referring to the ISO / IEC 27005: 2018 guide to practice in managing risks to information risk. ISO/IEC 27005 itself is part of the ISO 27000 series which includes guidelines for the implementation of an Information Security Management System (ISMS). The purpose of this research is to identify potential threats arising from information security controls from ISO / IEC 27002: 2022 that have not been fulfilled by PT XYZ for the next risk assessment stage on the main potential threats. The results of the risk assessment process obtained 7 potential threats which then for each threat proposed a form of risk control and action plan. The results of this study can be used as a reference for analyzing corporate information risk management, especially for risk threats arising from non-fulfillment of security controls in the ISO / IEC 27001 standard.

I. PENDAHULUAN

DALAM era digitalisasi yang semakin berkembang pesat saat ini, organisasi modern tidak dapat menghindari eksistensi risiko dalam berbagai aspek operasionalnya. Risiko adalah bagian alami dari setiap kegiatan bisnis, dan pengelolaannya menjadi kunci untuk menjaga efektivitas dan efisiensi proses organisasi, seperti yang disebutkan oleh Paul Hopkin dalam bukunya "Fundamental of Risk Management"[1]. Oleh karena itu, manajemen risiko telah menjadi aspek yang sangat penting dalam dunia bisnis. Salah satu bidang yang rentan terhadap risiko adalah Teknologi Informasi (TI) yang mendukung operasional perusahaan. Unit TI

merupakan aset berharga yang memerlukan perlindungan khusus, terutama dalam menjaga kerahasiaan, keutuhan, dan ketersediaan informasi (*Confidentiality, Integrity & Availability*)[2].

PT Nusantara Turbin Dan Propulsi, sebuah perusahaan teknik yang bergerak di bidang perawatan turbin gas dan peralatan berputar, juga memiliki unit TI yang sangat penting untuk mendukung proses bisnisnya. Namun, dengan semakin kompleksnya ancaman siber dan peraturan yang semakin ketat seperti PERMEN BUMN NOMOR PER-2/MBU/03/2023, perusahaan ini dihadapkan pada tantangan yang signifikan dalam mengelola risiko keamanan informasi. Identifikasi ancaman dan kerentanan pada aset TI menjadi suatu keharusan. Manajemen risiko, khususnya manajemen risiko keamanan informasi, adalah suatu proses yang mencakup identifikasi, analisis, penilaian, pengendalian[3], dan upaya menghindari risiko yang tidak dapat diterima [4]. Fokus utama dalam manajemen risiko keamanan informasi adalah menjaga kerahasiaan, keutuhan, dan ketersediaan informasi. ISO/IEC 27005:2018 memberikan panduan untuk manajemen risiko keamanan informasi, terutama dalam mendukung persyaratan Sistem Manajemen Keamanan Informasi (SMKI) sesuai dengan ISO/IEC 27001. Standar ini memberikan panduan langkah demi langkah tentang cara melakukan analisis dan evaluasi risiko keamanan informasi [6].

Meskipun ISO/IEC 27005:2018 memberikan panduan yang cukup rinci, pendekatan dalam manajemen risiko keamanan informasi masih bergantung pada konteks organisasi dan sektor industri (Ariyani & Sudarma, 2016). Oleh karena itu, masih ada kebutuhan untuk penelitian yang lebih spesifik dan terfokus pada praktik terbaik dalam manajemen risiko keamanan informasi, terutama dalam konteks PT Nusantara Turbin Dan Propulsi. Penelitian ini bertujuan untuk membantu Departemen Manajemen Informasi PT Nusantara Turbin Dan Propulsi dalam menilai tingkat risiko pada aset TI mereka berdasarkan ketidakterpenuhan kontrol keamanan informasi ISO/IEC 27002:2022. Selain itu, penelitian ini juga akan memberikan rekomendasi berupa praktik terbaik yang dapat diimplementasikan untuk menjaga keamanan informasi dengan langkah-langkah mitigasi terhadap potensi ancaman yang telah dinilai. Dengan demikian, penelitian ini diharapkan dapat membantu organisasi dalam meningkatkan pengelolaan risiko keamanan informasi mereka dan mematuhi peraturan yang berlaku, seperti PERMEN BUMN NOMOR PER-2/MBU/03/2023.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan tahapan yang telah terstruktur dan terorganisir. Tahap inisiasi melibatkan perumusan masalah, penentuan tujuan penelitian, dan studi literatur untuk merumuskan topik penelitian[7]. Tahap pengumpulan data melibatkan pengumpulan data primer melalui wawancara semi-terstruktur dengan pegawai Departemen MIS PT Nusantara Turbin dan Propulsi serta pengumpulan data sekunder berupa daftar aset dan risk register perusahaan. Pengolahan data dilakukan dengan cara pengkurasian data, yang melibatkan pemilihan, penyederhanaan, abstraksi, dan transformasi data mentah sesuai kebutuhan penelitian. Hasil pengolahan data digunakan sebagai panduan untuk fase identifikasi risiko, yang mencakup aset, ancaman, kontrol yang ada, dan konsekuensi potensial. Selanjutnya, dilakukan tahap risk assessment berdasarkan metodologi ISO/IEC 27005:2018:2018. Proses ini mencakup menentukan konteks, identifikasi risiko, menilai probabilitas dan dampak, serta verifikasi dan validasi hasil risk assessment. Setelah itu, dilakukan penarikan kesimpulan dan penyusunan rekomendasi untuk pengelolaan risiko keamanan informasi. Pada tahap evaluasi, hasil penelitian akan divalidasi oleh stakeholder perusahaan untuk memastikan kecocokan dengan kebutuhan PT Nusantara Turbin dan Propulsi. Metode evaluasi ini memastikan bahwa analisis risiko dan rekomendasi yang dihasilkan dapat diimplementasikan dengan efektif dalam konteks perusahaan.

A. Keamanan Informasi

Keamanan informasi adalah upaya untuk menjaga atau melindungi aset informasi dengan memperhatikan aspek kerahasiaan(confidentiality), integritas (integrity), dan ketersediaan(availability) terhadap ancaman yang mungkin timbul sehingga keamanan informasi dapat menjamin keberlangsungan proses bisnis, mengurangi risiko dan mengoptimalkan kinerja suatu perusahaan atau organisasi [8].

Kerahasiaan mengacu pada perlindungan informasi agar tidak diakses oleh pihak yang tidak berwenang. Dengan kata lain, hal ini memastikan bahwa hanya mereka yang memiliki izin yang diperlukan yang dapat mengakses informasi tertentu. Integritas melibatkan pemeliharaan konsistensi, akurasi, dan kepercayaan data di seluruh siklus hidupnya. Data tidak boleh diubah dalam perjalanan dan langkah-langkah harus diambil untuk memastikan bahwa data tidak dapat diubah oleh orang yang tidak berwenang. Ketersediaan memastikan bahwa informasi dapat diakses dan digunakan sesuai permintaan oleh pihak yang berwenang. Hal ini melibatkan pemeliharaan perangkat keras dengan benar, melakukan perbaikan perangkat keras segera ketika diperlukan, dan menjaga lingkungan sistem operasi yang berfungsi dengan benar [9].

B. SMKI

SMKI adalah pendekatan sistematis untuk menetapkan, menerapkan, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan keamanan informasi organisasi untuk mencapai tujuan bisnis. Hal ini didasarkan pada penilaian risiko dan tingkat penerimaan risiko organisasi yang dirancang untuk menangani dan mengelola risiko. Menganalisis persyaratan untuk perlindungan aset informasi dan menerapkannya dengan kontrol yang tepat untuk memastikan perlindungan aset informasi ini, sebagaimana diperlukan, berkontribusi pada keberhasilan implementasi SMKI [10].

C. ISO/IEC 27005

ISO/IEC 27005:2018 adalah standar internasional yang menyediakan pedoman Manajemen Risiko keamanan informasi. Standar ini membangun konsep pengetahuan, model, proses untuk membantu implementasi dengan mengambil pendekatan manajemen risiko [11]. Tugas-tugas dalam ISO27005 meliputi identifikasi, penilaian, dan penentuan prioritas risiko yang dilakukan dalam bentuk suatu proses berulang tanpa henti yang terdiri dari fase yang, jika diterapkan dengan benar, memungkinkan perbaikan dalam pengambilan keputusan dan peningkatan kinerja [12].

D. ISO/IEC 27002

Persyaratan yang dikodifikasikan dalam ISO 27001 diperluas dan dijelaskan dalam ISO 27002 dalam bentuk pedoman. Dengan pengembangan ISO 27002, praktik umum atau sering juga dikenal sebagai best practices ditawarkan sebagai prosedur dan metode yang terbukti dalam praktiknya, yang dapat yang dapat disesuaikan dengan persyaratan khusus dalam Perusahaan [13]. Pada pedoman ISO/IEC 27002:2022 diperkenalkan adanya jenis atribut kontrol. Dampak kontrol terhadap risiko tertentu dievaluasi menggunakan atribut control type. Tiga nilai dari atribut tersebut adalah preventive, detective, dan corrective. Tipe kontrol mendefinisikan kontrol mengenai waktu insiden keamanan informasi:

1) Preventive mengacu pada kontrol yang bertindak sebelum insiden terjadi.
2) Detective mengacu pada kontrol yang bertindak ketika sebuah insiden terjadi.
3) Corrective mengacu pada kontrol yang bertindak setelah insiden terjadi [14].

II. HASIL DAN PEMBAHASAN

A. Penetapan Konteks

Penetapan konteks adalah penetapan kriteria penting untuk manajemen keamanan informasi. Dalam penetapan konteks menjelaskan ruang lingkup dan batasan risiko yang disesuaikan berdasarkan tingkat keamanan informasi tingkat keamanan informasi yang ingin dicapai [15]. Penilaian yang dilakukan yaitu pada infrastruktur teknologi informasi di PT XYZ. Infrastruktur IT yang akan dibahas berdasarkan data yaitu aset-aset yang krusial seperti pada perangkat keras (hardware), perangkat lunak (software), dan arsip vital perusahaan. Pada penetapan konteks dilakukan pengelompokkan aset sebagai penentuan nilai aset. Kemudian, penentuan kriteria perhitungan dalam melakukan penilaian berupa analisis tingkat kemungkinan terjadinya risiko saat ini dan dampaknya terhadap aset perusahaan.

B. Identifikasi Aset

Aset perusahaan merupakan sumber daya yang mempunyai peran vital bagi keberlangsungan bisnis. Setiap perusahaan sudah pasti memiliki aset yang dianggap memiliki nilai dan digunakan untuk menunjang agar setiap kegiatan operasional perusahaan bisa berlangsung dengan lancar. ISO/IEC 27005:2018 memberikan panduan dalam melakukan identfikasi aset mengklasifikasikan aset menjadi 2 kategori yaitu aset utama dan pendukung [11]. Hasil Identifikasi Aset yang sudah dilakukan ditunjukkan pada Tabel I

C. Identifikasi Ancaman Utama

Identifikasi ancaman utama didapat dengan melakukan wawancara narasumber perusahaan untuk menentukan skenario ancaman mana saja yang perlu untuk menjadi prioritas pengananan risiko. Hasil Identifikasi ancaman utama yang sudah dilakukan ditunjukkan pada Tabel II

D. Pengelompokan Ancaman Berdasarkan Jenis Aset

Berdasarkan ancaman yang telah diidentifikasi, selanjutnya akan dilakukan pengelompokan ancaman yang telah disesuaikan dengan masing-masing aset IT. Pengelompokan ancaman ini bertujuan untuk memetakan aset apa yang mungkin dapat terdampak oleh suatu skenario ancaman. Pengelompokan dilakukan sesuai dengan aset utama dan aset pendukung . Adapun hasil pengelompokan ancaman terhadap asset ditunjukkan pada Tabel III

E. Evaluasi Risiko

Evaluasi risiko memiliki tujuan yaitu untuk membuat keputusan tentang risiko yang dievaluasi, termasuk keputusan apakah suatu tindakan apa yang harus dilakukan untuk risiko tersebut dan mana yang harus diprioritaskan untuk perlakuan risiko. Hasil evaluasi risikoyang telah dilakukan ditunjukkan pada Tabel V, V, VI, VII

F. Pengendalian Risiko

Pengendalian risiko adalah proses untuk mengelola risiko yang telah diidentifikasi dan dianalisis. Tujuan dari pengendalian risiko adalah untuk menentukan bentuk pengendalian risiko secara garis besar guna mengurangi kemungkinan risiko terjadi atau dampak negatif dari terjadinya risiko, sehingga perusahaan dapat mengelola risiko dengan lebih baik. Hasil dari pengendalian resiko yang telah diidentifikasi dan analisis ditunjukkan pada Tabel VIII

Hasil penelitian ini menunjukkan bahwa PT XYZ telah melakukan serangkaian langkah yang komprehensif dalam manajemen risiko keamanan informasi. Langkah pertama adalah identifikasi aset-aset krusial yang berperan penting dalam operasional perusahaan. Ini mencakup aset-aset utama seperti Proses Bisnis dan Informasi, serta aset-aset pendukung seperti Hardware, Software, Network, Personnel, dan Organization. Identifikasi ini penting karena membantu perusahaan dalam memahami dan mengakui nilai dari setiap aset yang perlu dilindungi. Selanjutnya, PT XYZ berhasil mengidentifikasi ancaman-ancaman utama yang dapat membahayakan keamanan informasi dan aset perusahaan. Ancaman-ancaman ini telah dikelompokkan berdasarkan kontrol yang relevan, jenis ancaman, dan ID yang sesuai. Dengan cara ini, perusahaan dapat mengidentifikasi ancaman yang paling signifikan dan mengutamakan langkah-langkah pengendalian yang tepat. Selama proses pengelompokan ancaman terhadap aset, PT XYZ mampu memetakan potensi dampak risiko pada setiap jenis aset. Pengelompokan ini membantu dalam memahami bagaimana skenario ancaman tertentu dapat berdampak pada aset-aset yang berbeda. Dengan pemahaman ini, perusahaan dapat merancang strategi pengelolaan risiko yang lebih terarah.

Evaluasi risiko adalah langkah berikutnya, dan PT XYZ telah berhasil mengevaluasi risiko untuk berbagai jenis aset, termasuk aset utama, Hardware, Network, dan Software. Evaluasi ini mencakup tingkat risiko yang berbeda-beda sesuai dengan jenis ancaman yang diidentifikasi. Ini memberikan pemahaman yang lebih mendalam tentang seberapa besar potensi risiko yang dihadapi oleh perusahaan, yang kemudian dapat digunakan untuk mengambil keputusan yang lebih baik dalam manajemen risiko. Terakhir, PT XYZ telah menetapkan pengendalian risiko yang sesuai berdasarkan tingkat risiko yang dievaluasi. Pengendalian ini mencakup respons risiko dan langkah-langkah konkret yang harus diambil untuk mengurangi risiko. Ini adalah langkah proaktif yang penting untuk melindungi aset perusahaan dan menjaga keamanan informasi. Dalam analisis gap, meskipun terdapat perbedaan dalam konteks dan metode yang digunakan dalam penelitian sebelumnya, kesamaan utamanya terletak pada penggunaan ISO/IEC 27005:2018 sebagai pedoman utama dalam manajemen risiko keamanan informasi. Dengan kata lain, semua penelitian ini mempercayai bahwa ISO/IEC 27005:2018 adalah kerangka kerja yang efektif untuk mengelola risiko keamanan informasi. Oleh karena itu, PT XYZ telah mengikuti praktik terbaik dalam industri ini dengan mengacu pada pedoman ini untuk mengelola risiko keamanan informasi mereka, yang sesuai dengan temuan-temuan dalam penelitian sebelumnya yang menggunakan pendekatan yang serupa.

Adapun untuk hasil identifikasi aset yang dimiliki perusahaan ada pada Tabel 1 berdasarkan 2 kategori aset yaitu aset utama dan pendukung. Aset utama yaitu aset yang berupa proses bisnis dan aktivitas, serta informasi yang sangat penting bagi organisasi. Sedangkan aset pendukung merupakan aset yang memiliki kerentanan sehingga dapat dieksploitasi oleh suatu ancaman yang mempengaruhi aset utama dalam lingkup organisasi.

TABEL I
IDENTIFIKASI ASET

Aset	**Jenis**
Aset Utama	Proses Bisnis
	Informasi
Aset Pendukung	*Hardware*
	Software
	Network
	Personnel
	Organization

TABEL II
IDENTIFIKASI ANCAMAN UTAMA

Aspek	Kontrol	Jenis Ancaman	ID
Organizational	*Independent review of information security.*	*Compromise of information*	T15
	Compliance with policies, rules, and standards for information security.	*Unauthorized actions*	T16
		Unauthorized actions	T17

	Assessment and decision on information security events.	*Unauthorized actions*	T7
	Privacy and protection of PII.	*Compromise of information*	T14
People	*Responsibilities after termination or change of employment*	*Unauthorized actions*	T24
Physical	*Cabling Security*	*Unauthorized actions*	T28
Technological	*Application security requirements*	*Unauthorized actions*	T31

Tabel II merupakan penjabaran mengenai skenario ancaman mana saja yang perlu untuk menjadi prioritas penganan risiko berdasarkan hasil wawancara narasumber.

TABEL III
PENGELOMPOKAN ANCAMAN TERHADAP ASET

Jenis Aset	ID	Kontrol	Jenis Ancaman
Aset Utama	T15	*Independent review of information security*	*Compromise of information*
	T14	*Privacy and protection of PII*	*Compromise of information*
	T17	*Compliance with policies, rules, and standards for information security*	*Unauthorized actions*
	T7	*Assessment and decision on information security events*	*Unauthorized actions*
	T24	*Responsibilities*	*Unauthorized actions*
	T31	*Technological*	*Unauthorized actions*
Aset Pendukung (*Hardware)*	T28	*Physical*	*Unauthorized actions*
	T15	*Independent review of information security*	*Compromise of information*
Aset Pendukung (*Network)*	T28	*Physical*	*Unauthorized actions*
Aset Pendukung (*Software)*	T16	*Compliance with policies, rules, and standards for information security*	*Unauthorized actions*
	T29	*Cabling Security*	*Unauthorized actions*
	T15	*Independent review of information security*	*Compromise of information*

Pada Tabel III di uraikan mengenai pengelompokan ancaman yang bertujuan untuk memetakan aset apa yang mungkin dapat terdampak oleh suatu skenario ancaman.

TABEL IV
EVALUASI RISIKO ASET UTAMA

ID	Jenis Ancaman	Tingkat Risiko
T15	*Independent review of information security*	12
T14	*Privacy and protection of PII*	12
T17	*Compliance with policies, rules, and standards for information security*	5
T7	*Assessment and decision on information security events*	9
T24	*Responsibilities*	15
T31	*Technological*	8

Tabel IV menunjukan tingkat risiko pada ancaman yang mempengaruhi aset aset utama

TABEL V
EVALUASI RISIKO ASET PENDUKUNG HARDWARE

ID	Jenis Ancaman	Tingkat Risiko
T28	*Physical*	8
T15	*Independent review of Information Security*	10

Tabel V menunjukan tingkat risiko pada ancaman yang mempengaruhi aset pendukung *hardware.*

TABEL VI
EVALUASI RISIKO ASET PENDUKUNG NETWORK

ID	Jenis Ancaman	Tingkat Risiko
T28	*Physical*	8

Tabel VI menunjukan tingkat risiko pada ancaman yang mempengaruhi aset pendukung *network*.

TABEL VII
EVALUASI RISIKO ASET PENDUKUNG SOFTWARE

ID	Jenis Ancaman	Tingkat Risiko
T16	*Compliance with policies, rules, and standards for information security*	9
T29	*Cabling Security*	8
T15	*Independent review of information security*	12

Tabel VII menunjukan tingkat risiko pada ancaman yang mempengaruhi aset pendukung *software*.

TABELVIII
PENGENDALIAN RESIKO

ID	Tingkat Risiko	*Risk Response*	Pengendalian Risiko
Aset Utama			
T15	12	*Risk Mitigate*	Dilaksanakannya audit khusus terkait SMKI berbasis ISO 27007
T14	12	*Risk Mitigate*	Adanya kebijakan mengenai perlindungan PII yang wajib dipatuhi seluruh *stakeholder* perusahaan
T17	5	*Risk Accept*	Risiko dinilai dapat terkendali berdasarkan tingkat risiko yang sesuai dengan risk tolerance dari perusahaan
T15	12	*Risk Mitigate*	Dilaksanakannya audit khusus terkait SMKI berbasis ISO 27007
T14	12	*Risk Mitigate*	Adanya kebijakan mengenai perlindungan PII yang wajib dipatuhi seluruh *stakeholder* perusahaan
T17	5	*Risk Accept*	Risiko dinilai dapat terkendali berdasarkan tingkat risiko yang sesuai dengan risk tolerance dari perusahaan
Aset Pendukung (Hardware)			
T28	8	*Risk Mitigate*	Menerapkan prosedur untuk prinsip cabling security menurut kontrol ISO 27002.
T15	10	*Risk Mitigate*	Dilaksanakannya audit khusus terkait SMKI.
Aset Pendukung (*Network*)			
T28	8	*Risk Mitigate*	Menerapkan prosedur untuk prinsip cabling security menurut kontrol ISO 27002.
Aset Pendukung (*Software*)			
T16	9	*Risk Mitigate*	Adamya prosedur pemantauan terhadap kepatuhan kebijakan keamanan informasi.
T29	8	*Risk Mitigate*	Menerapkan prosedur untuk prinsip cabling security menurut kontrol ISO 27002.
T15	12	*Risk Transfer*	Dilaksanakannya audit khusus terkait SMKI berbasis ISO 27007.

Tabel VIII memberikan penjelasan mengenai rekomendasi bentuk pengendalian risiko sesuai dengan kategori dari *risk response* dari masing masing skenario risiko.

III. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa dari hasil penilaian risiko, pada aset utama terdapat 6 risiko yang memerlukan pengendalian. Aset hardware memiliki 2 risiko risiko yang memerlukan pengendalian. Aset *network* memiliki 1 risiko dengan yang memerlukan pengendalian. Aset software memiliki 3 risiko yang memerlukan pengendalian. Berdasarkan nilai risiko yang perlu dimitigasi terhadap masing-masing aset, maka dapat dilakukan rekomendasi penanganan sebagai kontrol yang dapat mengurangi tingkat kemungkinan ancaman terjadi dan dampaknya di masa depan.

DAFTAR PUSTAKA

[1] Hopkin, P. (2018, March 7). Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management.
[2] Yudha, F. I. S., & Gunadhi, E. (2016). Risk Assessment Pada Manajemen Resiko Keamanan Informasi Mengacu Pada British Standard ISO/IEC 27005 Risk Management. Jurnal Algoritma, 13(2), 333-340.
[3] Ramadhan, D. L., Febriansyah, R., & Dewi, R. S. (2020). Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ. *JURIKOM (Jurnal Riset Komputer)*
[4] Darma, E. (2018, January 25). Analisis Manajemen Risiko Dan Pengendalian Intern Pada Pengadaan Jasa Konstruksi (Studi Kasus Pengadaan Jasa Konstruksi Pada SKPD Di Lingkungan Pemerintah Provinsi Sumatera Barat). Jurnal Pembangunan Nagari, 2(2), 189. https://doi.org/10.30559/jpn.v2i2.39.
[5] EJoko Wibowo, E., & Kalamullah Ramli. (2022). Impact of Implementation of Information Security Risk Management and Security Controls on Cyber Security Maturity (A Case Study at Data Management Applications of XYZ Institute). Jurnal Sistem Informasi, 18(2), 1-17. https://doi.org/10.21609/jsi.v18i2.1146.
[6] Dr. Ir. Ni Wayan Sri Ariyani M.M., NI WAYAN SRI ARIYANI and Prof. Dr. Ir. Made Sudarma, M.A.Sc., Made Sudarma (2016) Implementation of the ISO-IEC 27005 In Risk Security Analysis of Management Information System. Journal of Engineering Research and Applications (IJERA), 8 (8). ISSN 2248-9622).
[7] S. Hevner, A; March, "Research essay design science in infor-mation," pp. 75–105, 2004.
[8] S. Jaya Putra, M. Nur Gunawan, A. Falach Sobri, J. Muslimin, Amilin and D. Saepudin, "Information Security Risk Management Analysis Using ISO 27005: 2011 For TheTelecommunication Company," 2020 8th International Conference on Cyber and IT Service Management (CITSM), Pangkal, Indonesia, 2020, pp. 1-5, doi: 10.1109/CITSM50537.2020.9268845.
[9] Meriah, I., & Arfa Rabai, L. B. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. Procedia Computer Science, 160, 85–92. https://doi.org/10.1016/j.procs.2019.09.447.
[10] *ISO/IEC 27000:2018. (2022, May 4)*. ISO.
[11] ISO/IEC 27005:2018. (2020, December 16). ISO.

[12] Agrawal, V. (2017, June). A Framework for the Information Classification in ISO 27005 Standard. 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud).
[13] Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 04(02), 92–100.
[14] *GLAVAN, A., GHEORGHICA, D., & CROITORU, V. (2023, July 3). MULTI-ACCESS EDGE COMPUTING ANALYSIS OF RISKS AND SECURITY MEASURES. REVUE ROUMAINE DES SCIENCES TECHNIQUES — SÉRIE ÉLECTROTECHNIQUE ET ÉNERGÉTIQUE, 68(2), 206–211.*
[15] Fikri, M. A., Putra, F. A., Suryanto, Y., & Ramli, K. (2019). Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency. Procedia Computer Science, 161, 1206–1215.